KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA

SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Jenjang Strata I pada Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Diajukan oleh:

Bias Giyanisis

Endah Sudarmilah, S.T., M.Eng.

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
JULI 2014

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA

Yang dipersiapkan dan disusun oleh :

Bias Giyanisis

L200 100 126

Telah disetujui pada :

Hari :

Tanggal :

Pembimbing I

Endah Sudarmilah, S.T., M.Eng.

NIK: 969

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal :

Mengetahui

Ketua Program Studi

Teknik Informatika

Heru Supriyono, S.T.,M.Sc.Ph,D

NIK : 970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI TEKNIK INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/VI/2014

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Teknik Informatika menerangkan bahwa :

Nama	:	BIAS GIYANISIS
NIM	:	L200100126
Judul	:	KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA
Program Studi	:	Teknik Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 7 Juli 2014

Biro Skripsi
Teknik Informatika

Fauzan Natsir, S.Kom

Turnitin Originality Report

KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA by Bias Giyanisis

From September 2014 (publikasi maret 2014)

Similarity Index	Similarity by Source	
12%	Internet Sources:	5%
	Publications:	0%
	Student Papers:	10%

Processed on 08-Jul-2014 10:49 WIT
ID: 438440419
Word Count: 2412

sources:

1 6% match (student papers from 05-Feb-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 393683804

2 2% match (Internet from 11-Oct-2010)
http://www.ex-trick.co.cc/2010/03/konsep-dasar-sql-injection.html

3 2% match (student papers from 11-Jun-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 434098515

4 2% match (student papers from 30-Jun-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 437305930

5 1% match (student papers from 15-Apr-2013)
Submitted to Colorado Technical University Online on 2013-04-15

6 < 1% match (Internet from 04-May-2011)
http://deddie.com/sql.html

7 < 1% match (Internet from 29-Apr-2014)
http://govcsirt.kominfo.go.id/download/SOP/SOP%20IH_Web%20Defacement(2).pdf

paper text:

KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA SKRIPSI

Disusun

4**sebagai salah satu syarat menyelesaikan Jenjang Strata I pada Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika Universitas**

KINERJA APLIKASI CLIENT SERVER UNTUK SISTEM INFORMASI TUMBUH KEMBANG BALITA

Bias Giyanisis

Teknik Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-Mail : **Giyanisisbias@gmail.com**

ABSTRAK

Pada saat ini *aplikasi web* merupakan sumber untuk mencari informasi secara *modern* yang berkembang sangat cepat. Dalam pembuatan *aplikasi web* tidak hanya sisi *desain* dan informasi yang perlu diperhatikan tetapi dalam aspek keamanan dan kinerja dari sebuah *aplikasi web* itu sendiri mempunyai peranan yang sangat penting. Keamanan sebuah *aplikasi web* timbul dari kebutuhan untuk melindungi data dan *aplikasi web* itu sendiri sedangkan kinerja pada aplikasi web perlu diperhatikan juga agar tidak *hang* pada saat diakses banyak pengguna.

Pengujian dilakukan dilakukan terhadap sistem informasi tumbuh kembang balita dengan menggunakan *tool* berupa *software* dan langkah-langkah tertentu yang digunakan untuk menguji keamanan dan performanya. Untuk melakukan analisis keamanan *software* yang digunakan adalah *Acunetix website vulnerability scanner* sedangkan pengujian *performance* dilakukan dengan aplikasi *Httpwatch* dan *JMeter*.

Berdasarkan hasil pengujian keamanan yang telah dilakukan diketahui bahwa keamanan sistem informasi tumbuh kembang balita belum dapat dikatakan aman, hal ini di tunjukkan dengan masih adanya halaman-halaman dengan tingkat kerentanan pada *level High* dengan ditemukannya *web alerts* berbahaya yang menampilkan kerentanan seperti *blind sql injection, xss, weak password, cookie stealing*, dimana kerentanan tersebut dapat dicegah dengan memberikan *filtering* karakter berbahaya pada *inputan user*, menggunakan *password* yang sukar ditebak dan menggunakan jalur pengiriman data yang terenkripsi dan pada sistem informasi tumbuh kembang balita halaman yang paling rawan terhadap serangan *attacker* ada pada halaman login.

Berdasarkan pengujian kinerja pada sistem informasi tumbuh kembang balita menggunakan *httpwatch* dan *jmeter average time* meningkat seiring bertambahnya jumlah user yang mengakses secara bersamaan, ketika pengujian menggunakan *jmeter* dengan 25 *user* terlihat *average time* halaman perkembangan membutuhkan waktu lebih lama dibandingkan halaman lain dengan *average time* 15732 *millisecond* untuk menyelesaikan *request* dengan *throughput* hanya 0,804415145 *request/second*, disarankan untuk melakukan *compress* terhadap *file* gambar (.jpg, .png), menghapus atau memperbaiki *file* yang terindikasi *broken link*.

Kata kunci : Sistem Informasi, keamanan Sistem Informasi, Performa Sistem Informasi, *Acunetix, JMeter*.

PENDAHULUAN

Keamanan dan kinerja merupakan sebuah pondasi yang sangatlah penting dalam membangun sebuah sistem informasi. Dimana tanpa adanya keamanan sistem informasi dapat diacak-acak dari sisi tampilan oleh *cracker* dan tidak hanya sampai disitu bahkan data yang ada didalam sistem informasipun dapat dicuri untuk suatu tindakan yang tidak bisa dipertanggungjawabkan, sedangkan sistem informasi tanpa ditunjang dengan kinerja yang baik akan menyebabkan terjadinya *hang* bahkan *error* yang nantinya akan membuat pengunjung merasa terganggu.

Sistem informasi tumbuh kembang balita merupakan aplikasi *client server* berbasis web yang didalamnya menampilkan informasi-informasi dalam tampilan website yang berkaitan dengan tampilan awal *(home), profil*e, data berat badan, data tinggi badan, data lingkar kepala, data perkembangan balita, halaman *contact* serta halaman login. Alamat Sistem informasi tumbuh kembang balita untuk pengujian keamanan yaitu http://www.posyandu123.0fees.us sedangkan untuk performance dengan alamat http://www.posyandu123.esy.es, walaupun terdapat perbedaan alamat namun substansi di dalam Sistem informasi tumbuh kembang balita tetap sama.

Penelitian ini dilakukan dengan melakukan pengujian keamanan sistem informasi menggunakan *software vulnerability scanner* dan menggunakan *software Performance test* untuk pengujian beban akses.

TELAAH PENELITIAN

Detty Metasari (2014) meneliti tentang keamanan pada *website* Universitas Muhammadiyah Surakarta yang memiliki alamat sebagai berikut, “ums.ac.id”,“fkip.ums.ac.id”,“ekonomi.ums.ac.id”,“teknik.ums.ac.id”,“hukum.ac.id”, “geografi.ums.ac.id”,“psikologi.ums.ac.id” ,“fai.ums.ac.id”,“kedokteran.ums.ac.id”,“fik.ums.ac.id”,“farmasi.ums.ac.id”,“fki.umc.ac.id” dan website “alumni.ums.ac.id”.

Berdasarkan hasil pengujian keamanan *website* Universitas Muhammadiyah Surakarta diketahui adanya *sub domain* fakultas yang memiliki kerentanan pada *level High* dengan ditemukannya *web alerts High* pada beberapa *website* fakultas dan *level Medium*. *level Low* hanya terdapat pada alamat ums.ac.id.

METODE PENELITIAN

Pada pengujian ini peneliti menggunakan beberapa *tools* yang dijalankan dengan langkah-langkah tertentu digunakan untuk menguji keamanan dan kinerja sistem informasi. Untuk melakukan analisis sistem informasi dari segi keamanan *software* yang digunakan adalah *Acunetix vulnerability scanner* dan menggunakan *software Jmeter Performance test* untuk pengujian kinerjanya.

HASIL PENELITIAN

1. **Pengujian keamanan**

Scaning vulnerability menggunakan *acunetix* terhadap sistem informasi tumbuh kembang balita dengan alamat http://posyandu123.0fees.us menunjukan kerentanan pada *level* 3 (*High*). Terdapat total 21 *alerts*, 10 kerentanan beserta url yang terpengaruh oleh masing–masing kerentanan

Dari hasil *scanning* menggunakan *acunetix* dilakukanlah analisis terhadap kerentanan pada sistem informasi tumbuh kembang balita berdasarkan jenis kerentanannya, pengujian yang dilakukan sebagai berikut :

1. *Blind SQL Injection*

Blind SQL Injetion merupakan kerentanan yang memungkinkan *attacker* mengubah pernyataan *SQL* dengan memanipulasi *input user* dengan karakter-karakter berbahaya ketika sistem informasi menerima input dari *attacker* yang dibuat kedalam sebuah pernyataan *SQL* dimana sistem informasi tidak mampu melakukan *filter* karakter berbahaya. Kerentanan berupa *blind sql injection* terdapat pada :

a) Halaman *login* dengan url : /cek_login.php

kerentanan halaman *login* terdapat pada *script* untuk memanggil *database username* dan *password* yang terdapat pada gambar 3.

```
if($op=="in"){
    $cek = mysql_query("SELECT * FROM tabel_user
    WHERE username='$username'
    AND password='$Passwordhash'");
```

Gambar 3 *Script /cek_login.php*

Blind sql injection menggunakan fungsi logika seperti logika *AND* atau *OR* untuk mengecoh fungsi logika pada sistem informasi yang rentan terhadap *blind sql injection*, dimana Logika *AND* akan menghasilkan nilai *TRUE* ketika ekspresi *TRUE AND TRUE* dihubungkan. Script pada gambar 3 menggunakan logika *AND* yang mana pada *form login* ketika *username* bernilai *TRUE* dan *password* bernilai TRUE maka akan menghasilkan nilai *TRUE* yang artinya *session* baru akan terbuka dengan menampilkan halaman *administrator*. Misalkan pada *form login* kolom user diberi inputan dengan sintak *admin' or '' = '*. Maka proses *query* yang terjadi akan menjadi seperti ini :

SELECT * FROM user WHERE username=’ admin' or '' = ' AND password=”;

Artinya proses logika *AND* menjadi tercemar oleh logika *OR* dan dengan SQL ini hasil *selection* akan selalu bernilai *TRUE*, sehingga *password* salahpun akan dianggap benar. Dan yang terjadi adalah *session* akan terbuka untuk *attacker* tanpa perlu tahu passwordnya. *Acunetix* memberikan rekomendasi untuk kerentanan *blind sql injection* seperti berikut :

Resiko :

- *Blind SQL Injection* memungkinkan seseorang dapat *login* ke dalam sistem tanpa harus memiliki *account*.
- Memungkinkan seseorang merubah, menghapus, maupun menambahkan data–data yang berada didalam *database*.
- Dan mematikan *database*, sehingga tidak bisa memberi layanan kepada web server.

Rekomendasi :

- Script harus bisa melakukan *filtering parameter* yang dapat digunakan untuk proses *Blind SQL Injection*.
- Membatasi panjang *input box*.
- Sembunyikan pesan-pesan *error* yang keluar dari *SQL Server* yang berjalan.

2. *Cross site scripting*

Cross site scripting merupakan kerentanan yang terjadi karena *server* tidak mampu memvalidasi juga *filter* terhadap *input* dari *user*. Pada sistem informasi tumbuh kembang balita kerentanan *cross site scripting* terdapat pada :

a) Kerentanan terjadi pada url yang menampung *parameter* Id_balita.

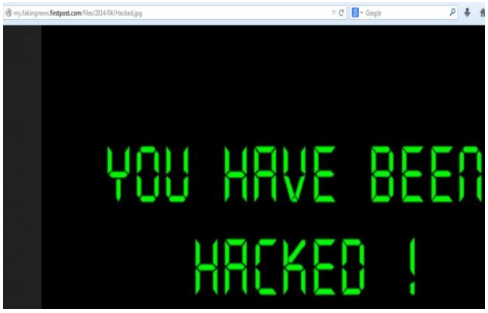
Acunetix scaning mendapati kerentanan terhadap *Cross Site Scripting* yang berpengaruh pada parameter "Id_balita", yang mana parameter Id_balita digunakan untuk menampilkan grafik pertumbuhan anak pada halaman pertumbuhan berat badan balita, pertumbuhan tinggi badan balita, dan pertumbuhan lingkar kepala balita, dimana pada halaman yang memakai parameter "Id_balita" menggunakan menggunakan *GET Method* yang memiliki kelemahan yakni terlihatnya *parameter* saat dilakukan pengiriman data *server* ke *client* atau sebaliknya yang terlihat di URL, seperti url "http://posyandu123.0fees.us/?proses=datk&id_balita=&id_balita=2&bln=0" yang menampilkan *parameter* seperti id_balita, proses=datk. Contoh *script* yang menggunakan *parameter* id_balita ditampilkan pada gambar 5.

```
$bln = $_GET['bln'];
$id_balita = $_GET['id_balita'];
```

Gambar 5 *script id_balita dengan GET Method*

Pengujian ditujukan pada halaman pertumbuhan lingkar kepala balita dengan alamat http://posyandu123.0fees.us/?proses=datk&id_balita=&id_balita=2&bln=0 , pada alamat halaman pertumbuhan lingkar kepala balita terlihat parameter-parameter yang digunakan untuk proses pemanggilan grafik pertumbuhan lingkar kepala balita yang rawan terhadap *xss*, penyerang dapat

melakukan penambahan parameter-parameter berbahaya untuk melakukan perusakan pada sistem informasi sistem tumbuh kembang balita, seperti penambahan parameter berikut. http://posyandu123.0fees.us/?bln=0&id_balita=2&id_balita=%27%20onmouseover%3dalert%28document.location=%27http://my.fakingnews.firstpost.com/files/2014/04/Hacked.jpg%27%29%20bad%3d%27&proses=datk, *parameter* yang ditambahkan menampilkan beberapa kode "*URL-encoding*" yang mana didalamnya berisi perintah ketika *mouse* bergerak melewati grafik pertumbuhan lingkar kepala balita maka akan muncul peringatan yang kemudian *client* diarahkan menuju halaman yang menampilkan "Hacked.jpg" yang terlihat pada gambar 5.



Gambar 5 *Hacked.jpg*

Rekomendasi untuk kerentanan *cross site scripting* sebagai berikut :

Resiko :

- Seorang *attacker* dapat melakukan pencurian terhadap *cookie*.
- Memungkinkan penyerang melakukan *deface* sistem informasi tumbuh kembang balita.

Rekomendasi :

- Melakukan *filtering* terhadap *metacharacter* dari inputan user.
- Menambahkan script blocking XSS setelah script " $id_balita = $_GET['id_balita']; ".

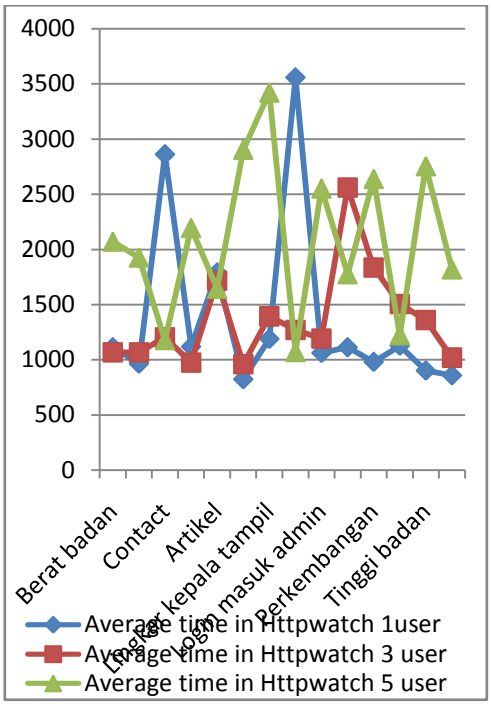
Script blocking XSS:

```
if(!ctype_digit($id_balita=$_GET['id_balita']))
{
echo "blocking XSS";
exit;
} else if($id_balita<=0)
{
echo "blocking XSS2";
exit;
}
```

2. Pengujian kinerja

Performance test dilakukan dengan memanfaatkan jaringan LAB-FKI untuk sistem informasi tumbuh kembang balita yang terdapat dalam posyandu123.esy.es. Semua halaman sistem informasi akan diuji dengan aplikasi *jmeter* dengan *virtual usernya* dan aplikasi *httpwatch* untuk mengukur *performa web* dengan *real user*, sehingga dapat diketahui halaman yang memiliki performa yang baik atau sebaliknya.

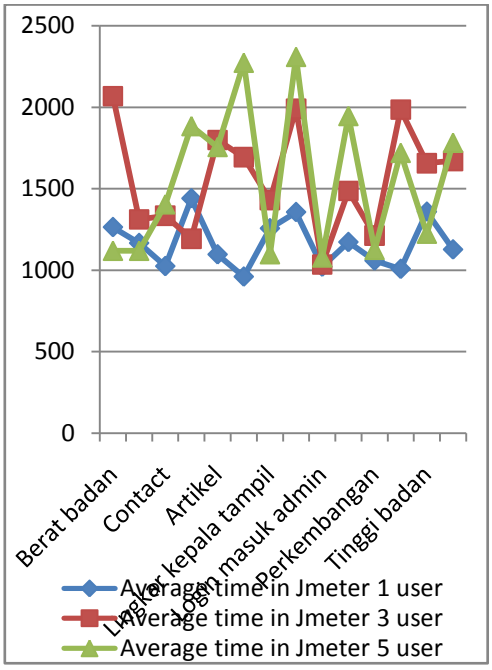
Average time menggunakan 1 user, 3 user, 5 user dengan httpwatch sebagai aplikasi pemcatat didapatkan grafik 1. berdasarkan grafik 1 terjadi peningkatan *average time* setelah dilakukan pengujian dari 1 user, 3 user hingga 5 user yang melakukan akses secara bersamaan namun tidak terlalu significant, terdapat pula perbedaan waktu rata-rata yang mencolok misalkan seperti halaman contact dan halaman login yang diakses oleh 1 user dimana membutuhkan rata-rata waktu yang lebih tinggi dibandingkan ketika diakses oleh 3 user dan 5 user, hal tersebut dimungkinkan karena adanya beberapa faktor yang mempengaruhi seperti *network*, banyak pengguna, data didalam sistem informasi.



Grafik 1 *average time httpwatch*

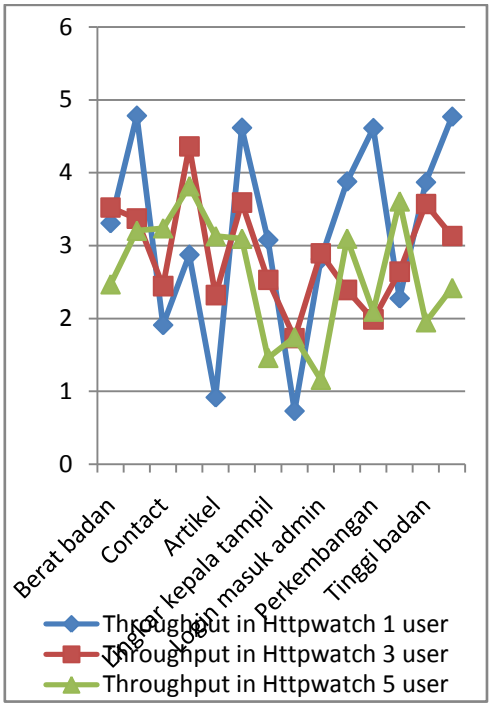
Average time pada *jmeter* menghasilkan grafik 2 dimana setiap halaman terjadi peningkatan ketika dilakukan akses dengan 1, 3, dan 5 *virtual user* seperti yang terjadi pada *real user* namun pada jmeter peningkatannya lebih stabil, saat dilakukan pengujian dengan 1 virtual user halaman yang memiliki rata-rata tertinggi adalah halaman home diikuti halaman login, ketika pengujian 3 virtual user rata-rata

waktu tertinggi terdapat pada halaman berat badan dan halaman login, dan pengujian dengan 5 *virtual user* menunjukan halaman login merupakan halaman yang memiliki rata-rata waktu terlama.



Grafik 2 *average time jmeter*

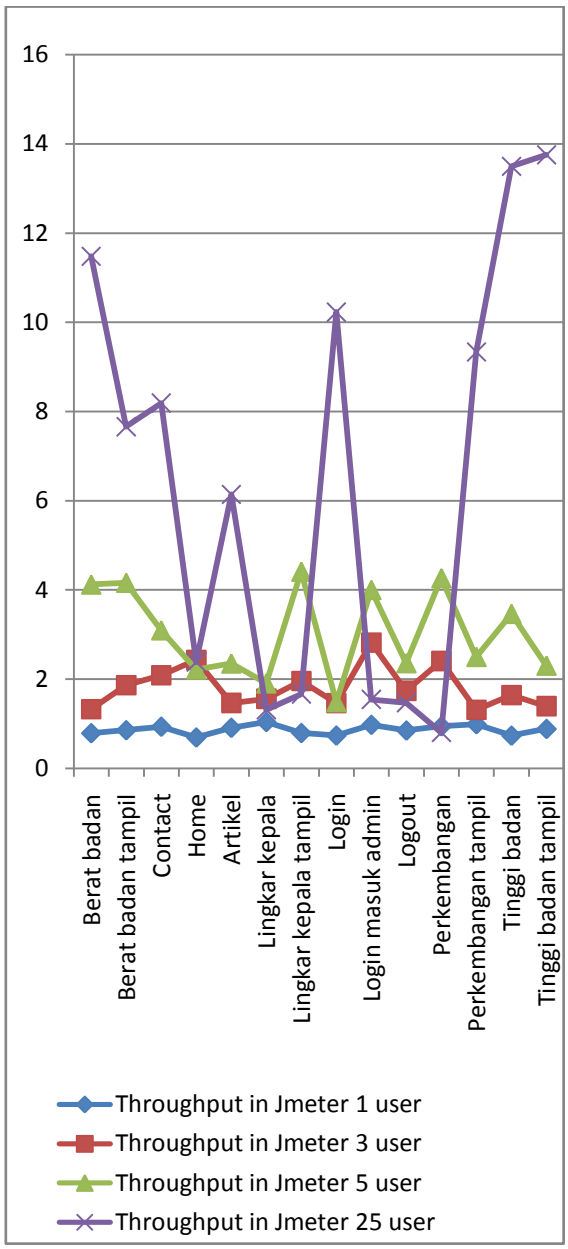
Httpwatch menampilkan hasil throughput dalam grafik 3 dimana throughput sistem informasi tumbuh kembang balita menunjukan antara angka 1 sampai 5 request/second dan hampir merata di setiap halaman, yang mana semakin tinggi angka throughput semakin bagus.



Grafik 3 *Throughput in httpwatch*

Pada grafik 4 tampak terjadi peningkatan throughput seiring bertambahnya jumlah *virtual user* yang melakukan akses ini menunjukan jumlah user merupakan salah satu faktor terjadinya peningkatan throughput namun perlu diperhatikan pula untuk *average* time sepertihalnya pada pengujian jmeter dengan 25 *virtual user* dimana hasil pada halaman perkembangan terjadi perbedaan yang mencolok halaman membutuhkan waktu rata-rata lebih lama dibandingkan dengan halaman lainnya dengan 15732 millisecond dan memiliki throughput paling rendah dengan

0,804415145 request/second, artinya *average time* memiliki korelasi dengan throughput yang mana hasilnya *average time* semakin kecil semakin baik dan semakin tinggi semakin baik pada throughput.



Grafik 4 *Throughput in JMeter*

Dari perbandingan *average time* dan *throughput* antara httpwatch dengan jmeter lamanya proses atau respon sistem informasi tumbuh kembang balita disebabkan karena banyaknya *file* dengan *format .jpg, .png* yang terlalu banyak dimana file gambar seharusnya bisa *dicompress* atau dikecilkan ukuranya agar tidak membebani sistem informasi, terdapat pula *file javascript* yang *brokenlink* yang seharusnya dapat diperbaiki agar tidak terjadi *error* atau bahkan menuju ke halaman lain ketika di akses, dan juga header dengan Get method yang memakan waktu banyak untuk menyelesaikan proses.

KESIMPULAN

Berdasarkan hasil pengujian keamanan yang telah dilakukan diketahui bahwa keamanan sistem informasi tumbuh kembang balita belum dapat dikatakan aman, hal ini di tunjukkan dengan masih adanya halaman-halaman dengan tingkat kerentanan pada *level High* dengan ditemukannya *web alerts* berbahaya yang menampilkan kerentanan seperti *blind sql*

injection, xss, weak password, cookie stealing, dimana kerentanan tersebut dapat dicegah dengan memberikan filtering karakter berbahaya pada inputan *user*, menggunakan password yang sukar ditebak dan menggunakan jalur pengiriman data yang terenkripsi dan pada sistem informasi tumbuh kembang balita halaman yang paling rawan terhadap serangan *attacker* ada pada halaman *login*. Berdasarkan pengujian kinerja pada sistem informasi tumbuh kembang balita menggunakan httpwatch dan jmeter *average time* meningkat seiring bertambahnya jumlah *user* yang mengakses secara bersamaan, ketika pengujian menggunakan jmeter dengan 25 *user* terlihat *average time* halaman perkembangan membutuhkan waktu lebih lama dibandingkan halaman lain dengan *average time* 15732 *millisecond* untuk menyelesaikan *request* dengan throughput hanya 0,804415145 *request/second*, disarankan untuk melakukan compress terhadap file gambar (.jpg, .png), menghapus atau memperbaiki file yang terindikasi *broken link*.

DAFTAR PUSTAKA

Anonim. “Apache JMeter - User's Manual Component Reference.” http://jmeter.apache.org/usermanual/component_reference.html (diakses tanggal 25 Mei 2014)

Anonim. “Apache JMeter - User's Manual Glossary.” http://jmeter.apache.org/usermanual/glossary.html (diakses tanggal 25 Mei 2014)

Qkye, Rezki. 2013. *Meminimalisasi Serangan Sql Injection*. http://rezkiiqkye.blogspot.com/2013/04/meminimalisasi-serangan-sql-injection.html (diakses tanggal 30 juni 2014)

Susanty, Yiyin, Widya & Ayu. 2012, *Pengujian Keamanan Sistem Web Server yang dikelola oleh PT. Web Architect Tecnology,* skripsi internship, Universitas Bina Nusantara, Jakarta.

Sutanta, Edhy 2008, *Analisis Keamanan Sistem Aplikasi (Study Kasus Aplikasi E-Learning di IST AKPRIND Yogyakarta),* skripsi, Institut Sains & Teknologi AKPRIND, Yogyakarta.

Tambun, Richson Untung. 2004. *CROSS SITE SCRIPTING*. Tugas Akhir. Teknik Elektro. Institut Teknologi Bamdung, Bandung.

Vacca, JR 2009. *Computer and Information Securty Handbook,* Elsevier, Inc, Wachington D.C.